

What is claimed is:

1 1. A system for dynamically identifying internal hosts in a
2 heterogeneous computing environment with multiple subnetworks, comprising:
3 an analysis module analyzing a plurality of packets, each such packet
4 comprising a source address of an originating host and a destination address of a
5 receiving host; and
6 a classification module classifying an unknown originating host located at
7 the source address of an outbound packet as an inside host with high confidence,
8 classifying an unknown receiving host located at the destination address of an
9 inbound packet as an inside host, and reclassifying the unknown receiving host as
10 an inside host with high confidence upon receiving a further outbound packet
11 having a source address corresponding to the address of the unknown receiving
12 host.

1 2. A system according to Claim 1, further comprising:
2 the classification module further classifying an unknown originating host
3 located at the source address of an inbound packet as an outside host.

1 3. A system according to Claim 2, further comprising:
2 the classification module reclassifying the unknown originating host as an
3 inside host with high confidence upon receiving an outbound packet having a
4 source address corresponding to the address of the unknown originating host.

1 4. A system according to Claim 1, further comprising:
2 the classification module further classifying an unknown receiving host
3 located at the destination address of an outbound packet as an outside host.

1 5. A system according to Claim 4, further comprising:
2 the classification module reclassifying the unknown receiving host as an
3 inside host with high confidence upon receiving an inbound packet having a
4 destination address corresponding to the address of the unknown receiving host.

1 6. A system according to Claim 1, further comprising:

2 the classification module maintaining the inside host with high confidence
3 classification of the unknown originating host upon receiving at least one of
4 further inbound packets and further outbound packets.

1 7. A system according to Claim 1, further comprising:
2 the classification module maintaining the inside host with high confidence
3 classification of the unknown receiving host upon receiving at least one of further
4 inbound packets and further outbound packets.

1 8. A system according to Claim 1, further comprising:
2 the classification module managing packet traffic flow by monitoring the
3 packets and adjusting control flow thereof.

1 9. A system according to Claim 8, further comprising:
2 the classification module ignoring packet traffic flow for each packet with
3 an originating host or a receiving host classified as an inside host with high
4 confidence.

1 10. A system according to Claim 1, wherein the packets are
2 communicated via a point-to-point protocol.

1 11. A system according to Claim 1, wherein the packets are
2 communicated via an end-to-end protocol.

1 12. A system according to Claim 1, wherein the packets are
2 communicated via the TCP/IP protocol and each source address and destination
3 address is an internet protocol (IP) address.

1 13. A method for dynamically identifying internal hosts in a
2 heterogeneous computing environment with multiple subnetworks, comprising:
3 analyzing a plurality of packets, each such packet comprising a source
4 address of an originating host and a destination address of a receiving host;
5 classifying an unknown originating host located at the source address of
6 an outbound packet as an inside host with high confidence;

7 classifying an unknown receiving host located at the destination address of
8 an inbound packet as an inside host; and
9 reclassifying the unknown receiving host as an inside host with high
10 confidence upon receiving a further outbound packet having a source address
11 corresponding to the address of the unknown receiving host.

1 14. A method according to Claim 13, further comprising:
2 classifying an unknown originating host located at the source address of
3 an inbound packet as an outside host.

1 15. A method according to Claim 14, further comprising:
2 reclassifying the unknown originating host as an inside host with high
3 confidence upon receiving an outbound packet having a source address
4 corresponding to the address of the unknown originating host.

1 16. A method according to Claim 13, further comprising:
2 classifying an unknown receiving host located at the destination address of
3 an outbound packet as an outside host.

1 17. A method according to Claim 16, further comprising:
2 reclassifying the unknown receiving host as an inside host with high
3 confidence upon receiving an inbound packet having a destination address
4 corresponding to the address of the unknown receiving host.

1 18. A method according to Claim 13, further comprising:
2 maintaining the inside host with high confidence classification of the
3 unknown originating host upon receiving at least one of further inbound packets
4 and further outbound packets.

1 19. A method according to Claim 13, further comprising:
2 maintaining the inside host with high confidence classification of the
3 unknown receiving host upon receiving at least one of further inbound packets
4 and further outbound packets.

1 20. A method according to Claim 13, further comprising:
2 managing packet traffic flow by monitoring the packets and adjusting
3 control flow thereof.

1 21. A method according to Claim 20, further comprising:
2 ignoring packet traffic flow for each packet with an originating host or a
3 receiving host classified as an inside host with high confidence.

1 22. A method according to Claim 13, wherein the packets are
2 communicated via a point-to-point protocol.

1 23. A method according to Claim 13, wherein the packets are
2 communicated via an end-to-end protocol.

1 24. A method according to Claim 13, wherein the packets are
2 communicated via the TCP/IP protocol and each source address and destination
3 address is an internet protocol (IP) address.

1 25. A computer-readable storage medium holding code for performing
2 the method according to Claims 13, 14, 15, 16, 17, 18, 19, 20 and 21.

1 26. A system for classifying hosts in a heterogeneous computing
2 environment, comprising:
3 a table storing records comprising a plurality of states which each specify
4 a location of a host relative to a network domain boundary, the states comprising:
5 an *Unknown* state describing an undefined host;
6 an *Outside* state describing a host located outside the network
7 domain boundary;
8 an *Inside* state describing a host provisionally located inside the
9 network domain boundary; and
10 an *Inside with High Confidence* state describing a host located
11 inside the network domain boundary;

12 a traffic manager classifying the hosts based on source address with each
13 outbound packet originating from an *Unknown* state, *Outside* state or *Inside* state
14 into an *Inside with High Confidence* state and classifying the hosts based on
15 destination address with each inbound packet originating from an *Unknown* state
16 or *Outside* state into an *Inside with High Confidence* state.

1 27. A system according to Claim 26, further comprising:
2 the traffic manager further classifying the hosts based on source address
3 with each inbound packet originating from an *Unknown* state into an *Outside*
4 state.

1 28. A system according to Claim 26, further comprising:
2 the traffic manager passing through packet traffic based on source address
3 with each inbound packet originating from an *Outside* state, *Inside* state or *Inside*
4 *with High Confidence* state and with each outbound packet originating from an
5 *Inside with High Confidence* state.

1 29. A system according to Claim 26, further comprising:
2 the traffic manager further classifying the hosts based on destination
3 address with each outbound packet originating from an *Unknown* state into an
4 *Outside* state.

1 30. A system according to Claim 26, further comprising:
2 the traffic manager passing through packet traffic based on destination
3 address with each outbound packet originating from an *Outside* state, *Inside* state
4 or *Inside with High Confidence* state and with each inbound packet originating
5 from an *Inside with High Confidence* state.

1 31. A system according to Claim 26, further comprising:
2 the traffic manager ignoring packet traffic based on source address or
3 destination address with each outbound packet and each inbound packet
4 originating from an *Inside with High Confidence* state.

1 32. A system according to Claim 26, wherein the heterogeneous
2 computing environment is IP compliant.

3 33. A method for classifying hosts in a heterogeneous computing
4 environment, comprising:

5 defining a plurality of states which each specify a location of a host
6 relative to a network domain boundary, the states comprising:

7 an *Unknown* state describing an undefined host;

8 an *Outside* state describing a host located outside the network
9 domain boundary;

10 an *Inside* state describing a host provisionally located inside the
11 network domain boundary; and

12 an *Inside with High Confidence* state describing a host located
13 inside the network domain boundary;

14 classifying the hosts based on source address with each outbound packet
15 originating from an *Unknown* state, *Outside* state or *Inside* state into an *Inside*
16 *with High Confidence* state; and

17 classifying the hosts based on destination address with each inbound
18 packet originating from an *Unknown* state or *Outside* state into an *Inside with*
19 *High Confidence* state.

1 34. A method according to Claim 33, further comprising:
2 classifying the hosts based on source address with each inbound packet
3 originating from an *Unknown* state into an *Outside* state.

1 35. A method according to Claim 33, further comprising:
2 passing through packet traffic based on source address with each inbound
3 packet originating from an *Outside* state, *Inside* state or *Inside with High*
4 *Confidence* state and with each outbound packet originating from an *Inside with*
5 *High Confidence* state.

1 36. A method according to Claim 33, further comprising:

2 classifying the hosts based on destination address with each outbound
3 packet originating from an *Unknown* state into an *Outside* state.

1 37. A method according to Claim 33, further comprising:
2 passing through packet traffic based on destination address with each
3 outbound packet originating from an *Outside* state, *Inside* state or *Inside with*
4 *High Confidence* state and with each inbound packet originating from an *Inside*
5 *with High Confidence* state.

1 38. A method according to Claim 33, further comprising:
2 ignoring packet traffic based on source address or destination address with
3 each outbound packet and each inbound packet originating from an *Inside with*
4 *High Confidence* state.

1 39. A method according to Claim 33, wherein the heterogeneous
2 computing environment is IP compliant.

1 40. A computer-readable storage medium holding code for performing
2 the method according to Claims 33, 34, 35, 36 and 37.